SECURED INFORMATION EXCHANGE IN SMART GRIDS

DEEPIKA BARIK (111EE0194)

DIBYARAJ KRISHNA BEHERA (111EE0197)

DEPARTMENT OF ELECTRICAL ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA-769008(ODISHA)

SECURED INFORMATION EXCHANGE IN SMART GRIDS

This project is submitted as a part of fulfilment of requirement for the degree of

Bachelor in technology in ***Electrical Engineering***

By

DEEPIKA BARIK-111EE0194

DIBYARAJ KRISNHA BEHERA-111EE0197

Under Guidance of

Prof. PRASANA KU. SAHU

DEPARTMENT OF ELECTRICAL ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY,

ROURKELA, ODISHA

7TH MAY 2015

CERTIFICATE

This is to certify that the thesis entitled as "**SECURED INFORMATION EXCHANGE IN SMART GRIDS**" submitted by **DEEPIKA BARIK(111ee0194) & DIBYARAJ KRISHNA BEHERA(111ee0197)** as a part of fulfilment of the requirements for the award of **Bachelor of Technology** in **Electrical Engineering** during session 2014-2015 at NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA. A bonafide record of research work carried out by them under my supervision and guidance.

The candidates have fulfilled all the prescribed requirements.

The Thesis which is based on candidates' own work, is not submitted elsewhere for any Degree/diploma.

In our opinion, the thesis is of standard required for the award of a bachelor of technology degree in Electrical Engineering.

Place: Rourkela

DEPARTMENT OF ELECTRICAL ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY,

ROURKELA, ODISHA

Dr. Prasan Ku.Sahu

Professor

ACKNOWLEDGEMENTS

We wish to express our sincere gratitude to PROF. Sunil Ku. SARANGI, Director and Prof. Anup Ku. PANDA, H.O.D of Electrical Engineering Department of National Institute of Technology, Rourkela for providing us an opportunity to do my project work on "SECURED INFORMATION EXCHANGE IN SMART GRID". This project bears on support of many peoples. I sincerely thank to my project guide Professor PRASANA KU. SAHU, Department of Electrical Engineering, National Institute of Technology, Rourkela for his able guidance and constant encouragement in carrying out this project work. Lastly we appreciate ours parents and friends for motivation and helping us to compete the project.

ABSTRACT

Smart Grid is a modernized electrical system that integrates power distribution with information technologies. To facilitate efficient and secure information exchange wireless networks must to be widely used in smart grid. The wireless communication network used here is one of major problem as it has raised issues of confidentiality and security of the utility and consumer and can lead to various attacks such as eavesdropping, information tampering, and jamming.

In present we use conventional wireless methods for exchanging all kinds of information of demand, protection system, tariff rate, customer details, safety details along with power quality data and event management data. This information has to be transmitted securely else the system can be vulnerable to third party interference or even more.

'Spread spectrum' technique is one of the method that can be used to prevent such attacks in wireless communication which also allows to achieve the privacy of information during transmission over the grids and gives us opportunity for dynamic control of the power system irrespective of the power flow direction.

Low probability of intercept and anti-jamming features are the inherent property of SS technique because of which the military system has used spread spectrum method for their communication for so many years.

SS signals are transmitted over the grids at a low spectral power density, i.e. bandwidth of the signal is increased keeping the amplitude and power of the signal constant, measured in watts per hertz. The use of Pseudo-Noise (PN) codes used in SS technique makes signal appear like noise and of high bandwidth.

The paper focuses on the different technology like Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) for secured exchange of information to ensure better QOS (Quality of Service) and reliability as well as to prevent any distortion in data at the receiver. Here we have simulated for both fhss and dsss and the results are shown.

CONTENTS:

LIST OF THE FIGURES:

ABBREVIATIONS USED IN PAPER:

i. SS- Spread Spectrum
ii. DSSS- Direct Sequence Spread Spectrum
iii. FHSS- Frequency hopping Spread Spectrum
iv. PN- Pseudo noise
v. SNR- Signal to Noise Ratio
vi. BPSK modulation- Binary Phase Shift Key modulation
vii. AMR- Automatic Meter Reading
viii. PLCC -Power Line Carrier Communication
ix. VVO- Voltage VAR Optimisation

CHAPTER 1

INTRODUCTION

1.1 Literature Survey and Motivation

Smart Grid is the advanced electrical power network that can be used to improve reliability, efficiency, economics and sustainability of generation, transmission distribution of electric energy using both digital and analog information of communication technology. Smart grid is the future technology of electrical network and considered to be next generation of the grid, as soon as we implement it will highly benefits us. China has already invested $61.4 billion on Smart Grid Market and US with $171.9 billion on Smart Grid and smart metering.

But with the increase of cybercrime on communication system, security concern of smart grid is highly important .The information shared between utilities and meters in consumer's house and industries, there is a chance of exploitation of information shared by other third parties and raised issues about privacy of consumers. Electricity theft is a concern all over the world, so we need to provide adequate security layers to Smart Grid for its safety. As India is growing in electricity market, so both government and academic institution should come up with ideas to implement Smart grid, and Smart Cities.

1.2 PROBLEM STATEMENT:

Bidirectional data flow of information is required in smart grid to create an automated and widely distributed network which also requires real time information to manage the electric power efficiently.

While transferring all this information from one grid to another if gets leaked to any other will make the power system vulnerable to jamming, third party interfering, even to terrorist attacks.

Normally we use wireless communications for sharing the information which can be tampered easily. So extra security measures must be taken to ensure secure transmission of information throughout the grids.

CHAPTER 2

SMART GRID

2. INTRODUCTION

2.1 What is a smart grid?

In general smart grid is the modernization of electrical power delivering system. This is an electrical network having capability to integrate the actions of utility and consumers in order to deliver sustainable electricity supply as well as secured connection between the utilities.

It provides a power system capable of two way communication as well as opportunity for real time monitoring and control. So, overall efficiency of the power system network is improved and also facilitates integration of renewable energy into the existing system. The limitations of the existing grid along with degradation in the power quality with significant increase in demand can be met with improvisation of the grids or smart grids. [1]

2.2 limitations of existing grid

- Less reliability: our overburdened grid has begun to fail us more frequently and presents us with substantial risks. Even as demand has increased; with less investment in energy generation further limits grid efficiency and reliability. A rolling blackout across Silicon Valley totalled $75million in losses.[2]
- Lower efficiency
- Inability of the generation system to meet higher demands
- High cost (owing to high fuel cost)
- Poor power quality
- Environment pollution : still 50% of the electricity is generated by burning coal and accounts for 25% of greenhouse gas generated.[2]
- Negligent to customers' choices
- Vulnerability to natural calamity and third party interference because of interconnection and concentrated network.

2.3 Main features of smart grid:

i. Intelligent
ii. Efficient
iii. Capable of accommodating energy from any source
iv. Real time monitoring and/or control to motivate consumers to control their energy consumption
v. Better power quality
vi. Resilient to interference and jamming
vii. Environment friendly
viii. Integrating renewable energy

2.4 **STRUCTURE OF SMART GRID:**

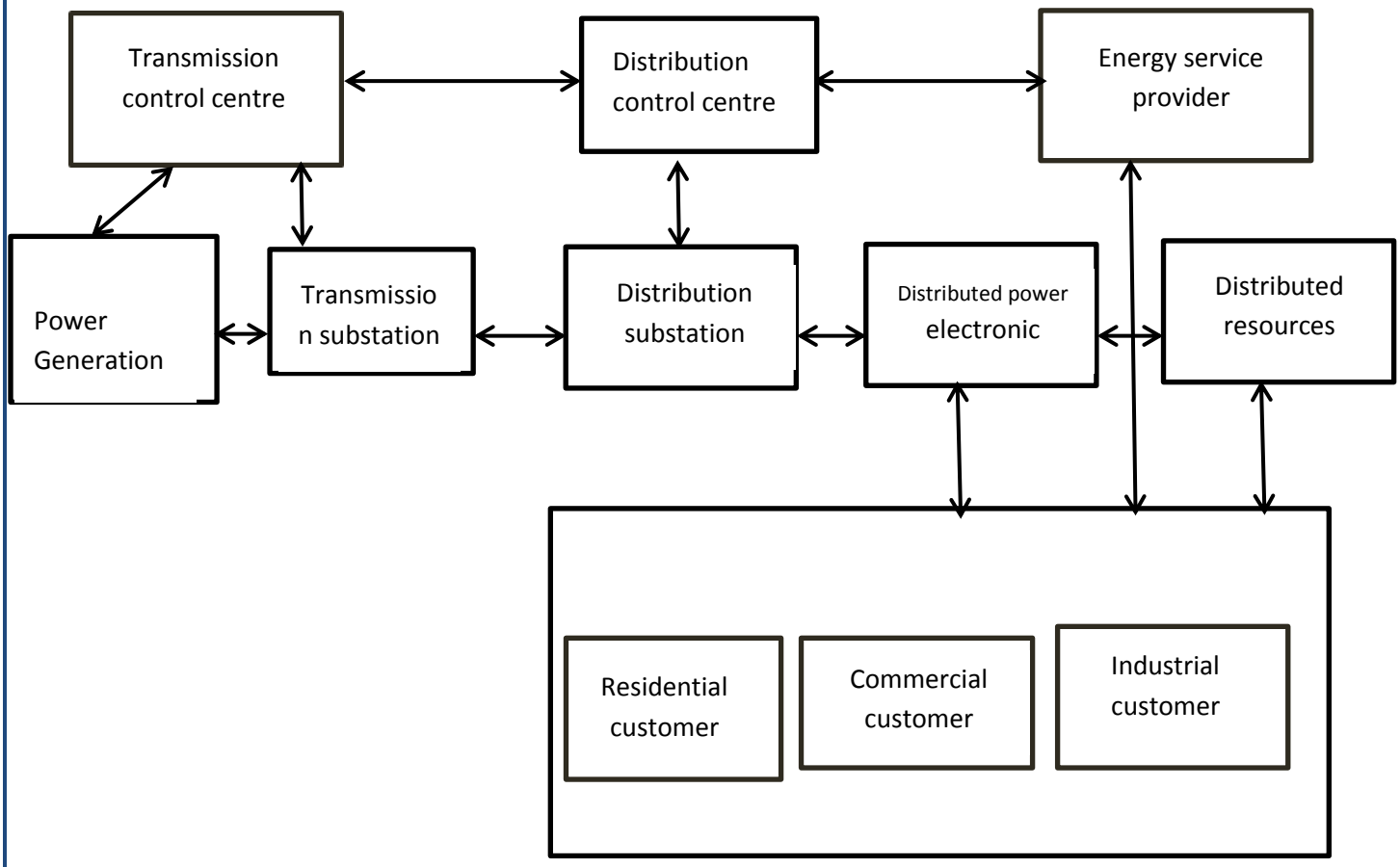

Fig 2.1

2.5 **ADVANTAGE OF SMART GRID**

a) Energy conservation and less environment pollution- Plug in Hybrid Vehicles and Electric Vehicles (EV) – substituting fuel sources in vehicles with renewable energy sources has the opportunity to lower CO_2 production. So we can plug in the vehicles at night which would have been generated anyway (and wasted), as a result it can also reduce CO_2 generation.[2].

b) It provides technology for Bi-directional flow of power as well as its monitoring in real time & information supply and demand balancing.[5]

c) It provides Automatic Meter Reading (AMR) from remote connection and load management.

d) Also it allows integration of Renewable energy resources to the system. It can avoid the running reserve system where less environmentally friendly power stations keep generators running so that they can meet sudden increase of load and it can be reduced with more predictable renewable sources.

e) It gives better choices for consumer to monitor and control their energy use so they can be more cautious.

f) It enhances the level of reliability and security of power generation and distribution.

g) It also improves the economy of the nation with efficient management of power supply.

h) Smart Grid uses technologies such as state estimation, fault detection, self-healing all this will lead to reliability and reduce vulnerability of attack.

i) Smart grid also provides load management from consumer side or demand side like turning off of air conditioners or thermal heaters during short term spikes in electricity price, reducing the voltage on distribution lines when possible through Voltage VAR Optimisation (VVO), eliminating truck roll for meter reading also avoids damages the devices which are sensitive towards the variation of the voltage.

j) Smart Grid also helps in peak curtailment i.e. reducing the demand during the high cost peak usage periods that could provide further benefits.[6]

CHAPTER 3

STRUCTURAL ANALYSIS

3. **STRUCTURAL ANALYSIS:**

3.1 **INFORMATION SHARED OVER SMARTGRIDS**

i. Smart metering data
ii. Operation event data
iii. Power quality details (voltage, frequency, power factor)
iv. Protection system fault data
v. Asset management data
vi. Demand response data
vii. Station maintenance data
viii. Engineering data
ix. Load profile recording
x. Pre-payment details
xi. Tariff plan details
xii. Customer specific tariff optimization data
xiii. Contact management details
xiv. Expense estimation
xv. Safety details
xvi. Load distribution data

3.2 **TECHNOLOGY USED**

This information is used in different utilities, generating stations, distribution stations in different systems like

i. SCADA (Supervisory Control And Data Acquisition)
ii. EMS (Emergency Management System)
iii. DMS (Distributed Management System)
iv. GIS (Geographical Information System)
v. SER (System event Recording)
vi. DFR (Digital Fault Recorder)

3.3 **RECENT COMMUNICATION SYSTEMS USED IN SMART GRIDS:**

3.3.1 PLCC Technique:

This method is used for bidirectional data communication between customer and the utility. But it has a small bandwidth which is not applicable for widely distributed network as in smart grids

3.3.2 ZIG BEE

It includes home automation and control, industrial real time monitoring, use of wireless sensors etc.

CHAPTER 4

SECURITY LAYER OF SMART GRID

4 **SECURITY LAYERS NEEDED IN SMART GRID**:

Smart grid communication system consists of different security layers such as follows

i. Physical security
ii. Equipment security
iii. Network security
iv. Application security
v. Information security

For secure transmission of the information for efficient use of the electrical energy, the communication must be encrypted in order to prevent third party interference and jamming. One of the various methods is spread Spectrum method.

This can be achieved by direct sequence spread spectrum i.e. DSSS and frequency hopping spread spectrum methods i.e. FHSS.

CHAPTER 5

SPREAD SPECTRUM (SS)

5 **SPREAD SPECTRUM**

SS is the widely used system for secure communication in Military communication. It allows a transmitter to transmit a message signal to a receiver end securely. In this method the bandwidth of the signal is increased in such a way that the message can't be detected by a receiver for whom it is not intended as the transmitted signal has a low power spectral density so that it lies below the noise level for third party. SS is used in satellite communication, police radar, and extra signals can be transmitted over the same bandwidth, thereby increasing the user. Here we increase the bandwidth of the signal deliberately to reduce the power density per frequency in order to make it difficult to monitor and hence difficult to interfere or jam.

5.1 INTRODUCTION

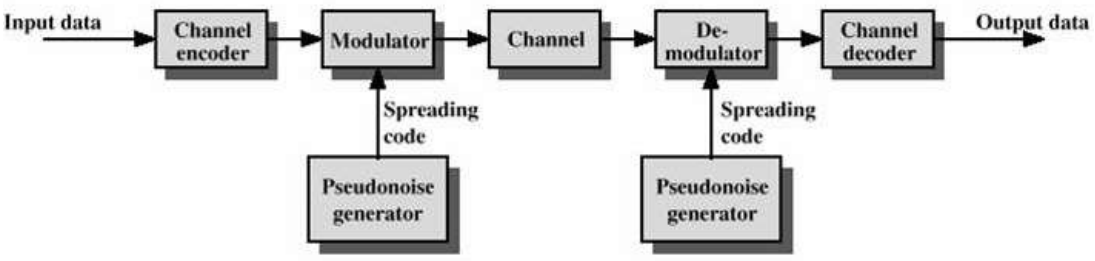

FIG 5.1: SPREAD SPECTRUM TECHNIQUE

5.2 HOW DOES SPREAD SPECTRUM (SS) WORK?

SS uses a pseudo-noise like signal to increase the bandwidth .Here the transmitted signal is spread over a wide frequency band, so that power content per frequency decrease and it becomes difficult to detect the signal. Also the spectral power density decreases below the thermal noise, so whenever someone try to interrupt/hack the signal, he will get only noise.

SS uses very high frequency (radio frequency) i.e. 10 kHz-1MHz for transmission and its bandwidth is increased for about more than 1000 fold. SS system develops its process gain in a sequential manner with bandwidth of the signal spreading and dispreading operation. The difference in SNR of input signal & output signal in any processor is called as its "process gain".

The advantage is obtained from this can be explained from **Claude Shannon's equation** describing channel capacity. [4]

$$C = W \log\left(1 + \frac{S}{N}\right)$$

Where; C=channel capacity, W=Bandwidth, S=signal power, and N=noise power.

From this equation we can conclude that by increasing the bandwidth of the signal, the signal to noise ratio decreases without any decrease in performance. The process gain (GP) increased the system performance, a high SNR is not required which can be explained mathematically as:

$GP = \frac{BWRF}{RINFO}$ Where; BWRF= Radio Frequency Bandwidth, RINFO= Information Rate

There are two types of the spread spectrum techniques

- **Direct-sequence spread spectrum- DSSS**
- **Frequency hopping spread spectrum- FHSS**

In DSSS the digital data is directly multiplied with pseudo random code to increase the bandwidth, PN sequence is only known to transmitter side and receiver side, In FHSS ,we change the carrier frequency for different time period over the channel.

5.3 **ADVANTAGE OF SS**

a. Interference is reduced.
b. Better quality of data processing
c. Lower susceptibility to multiple fading.
d. Harder to detect, demodulate and jams
e. Inherent security
f. Co-existence (less interference with each other)

CHAPTER 6

DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

6.1 INTRODUCTION

DSSS are the best known and most widely used spread spectrum techniques for communication process because system does not require a high speed, fast-settling frequency synthesizer which makes it easier to implement. Here modulation of a carrier by a code sequence called as Pseudo Random Code (PN sequence). This code looks like a noise signal but actually not random at all, so also called as white noise. Process gain in a direct sequence system is a function of the RF bandwidth of the signal transmitted, compared with the bit rate of the information .The gain in question is exhibited as a signal-to-noise improvement resulting from the RF-to-Bandwidth trade-off.[7]

6.2 PN SEQUENCE CODE GENERATOR:-

PN Sequence code generator is system in which it generates a random sequence number of 0 or 1. Normally flip flops with linear feedback serve the purpose.

- It increase the bandwidth of the signal , and it is randomness and unpredictable
- It is mainly used to increase the randomness and unpredictability of the signal.

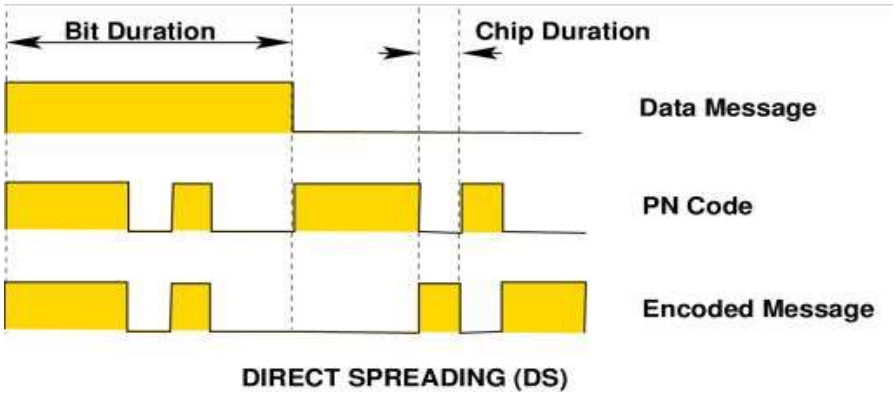

Fig (6.1) Direct Spreading

6.3 **STRUCTURAL AND MATHEMATICAL ANALYSIS OF DSSS**

6.3.1 **MODEL OF A DIRECT-SEQUENCE SPREAD BPSK SYSTEM**

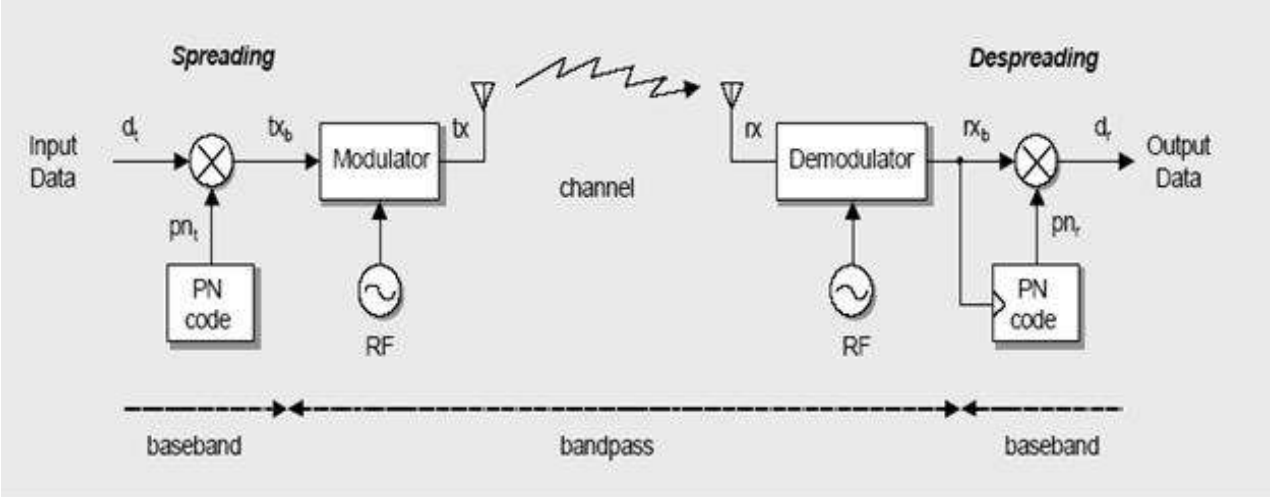

Fig 6.2

INPUT:-

- Binary data d_t with symbol rate of $R_s = 1/T_s$ (= bit rate R_b for BPSK)
- Pseudo Noise code pn_t with chip rate $R_C = 1/T_s$ (an integral multiple of R_S)

6.3.2 **SPREADING AND MODULATION IN DSSS:**

In DSSS we need to spread the data over a higher bandwidth before modulating. So first of all the input data is multiplied by a noise like signal (Pseudo noise) i.e. a binary signal with higher value at +1 and lower value at -1.

This PN code has a frequency which is approximately 1000 times that of the input signal. It produces the baseband signal as tx_b.

Where $tx_b = d_t \times pn_t$

Now the baseband signal has bandwidth = R_s

After spreading, the signal is modulation is done with a suitable carrier signal (sinusoidal) and transmitted over the channel. [8]

6.3.3 **DEMODULATION AND DESPREADING IN DSSS:**

The SS signal is not detected by any narrowband receiver. In the receiver side , the baseband signal r_{xb} is multiplied with the PN sequence pn_r to dispread the signal i.e. to decrease the bandwidth to its original value.

- If $pn_r = pn_t$ and synchronized to the PN sequence in the received data, then the binary data is recover on d_r; otherwise dispreading is not possible.

Then the sent information can be extracted from the signal using coherent carrier demodulation.

Binary Phase shift Key (BPSK) is used (without filtering) for both modulation and demodulation technique.

6. 4 MATHMATICAL ANALYSIS:

Input data signal represent : $\boldsymbol{d_t}$

PN code : $\boldsymbol{pn_t = pn_r}$

Carrier Signal : $\mathbf{A}\cos 2\pi f_c t$

Noise signal : $\boldsymbol{n_s}$

The transmitter output is given by: $t_x = d_t \,.\, pn_t(\mathbf{A}\cos 2\pi f_c t)$

The channel output is given by : $r_x = t_x + n_s = d_t \,.\, pn_t(\mathbf{A}\cos 2\pi f_c t) + n_s$

The demodulator output $\mathbf{rx_b}$: $r_{xb} = r_x.(\mathbf{A}\cos 2\pi f_c t)$

Despreading output $\mathbf{Z_r}$: $Zr = r_{xb}.pn_r = d_t\, pn_t^2 + n_s \,.\, pn_t = d_t + n_s \,.\, pn_t$

The original signal is recover at the receiver side by using the PN sequence code, it must to be properly synchronized at both transmitter and receiver end.

CHAPTER 7

FREQUENCY HOPPING SPREAD SPECTRUM (FHSS)

FREQUENCY HOPPING SPREAD SPECTRUM

7.1 INTRODUCTION

FHSS is the 2nd type of spread spectrum method we use; in this method frequency of the carrier jumps randomly from one frequency to another. Normally a frequency band from 2400MHz to 2483 Mhz is used for the purpose. As a result it is difficult to monitor and interfere with FHSS signal unless the person knows exactly the sequence of change of the hopped signal.

In this method frequency of the carrier remains constant for a mention period of time duration-this period is called as the hop period T_h .

When the whole channel is divided into different sub channels width of each sub channels represents the bandwidth of input. The sequence of hopping from one frequency to other frequencies is always fixed.

There is a set of different carrier frequencies called as the hop set. This hopping of frequency is typically done in pseudo manner.

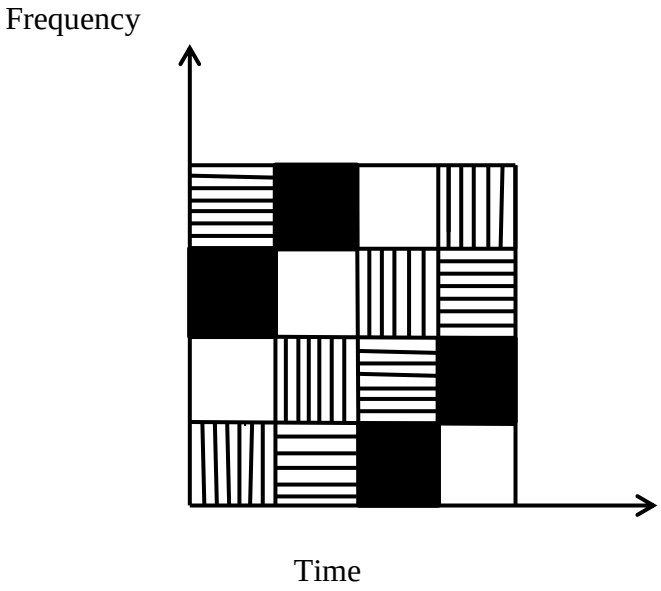

Fig 7.1: Hopping of Frequency

7.2. Slow and Fast FHSS:

In slow FHSS frequency of the carrier is set to be a value that carrier time period is greater than the hop period of the system. As a result it provides opportunity for coherent data detection and error controlling.

On the other hand in fast frequency hopping is done faster than the modulation of the signal. In this case data detection and modulation is more difficult than slow FHSS as it requires extremely fast carrier synchronization.

Diagram:

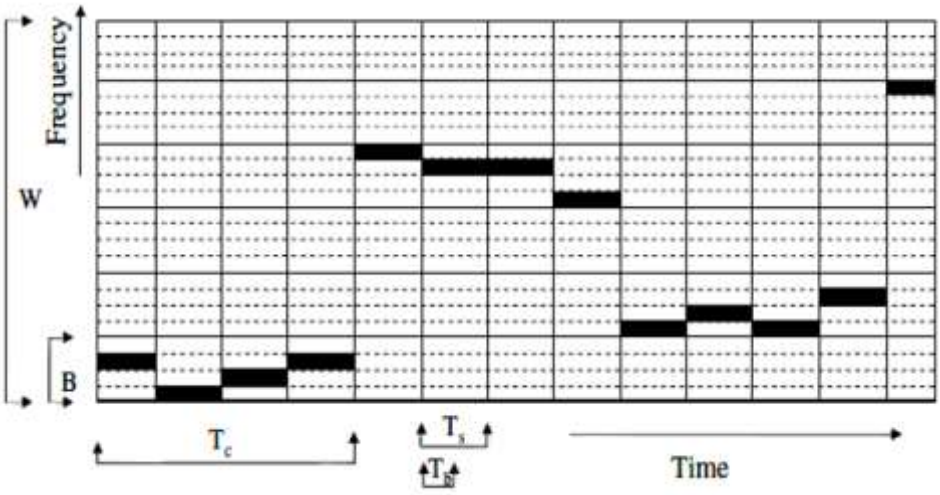

Fig 7.2: slow FHSS

Diagram:

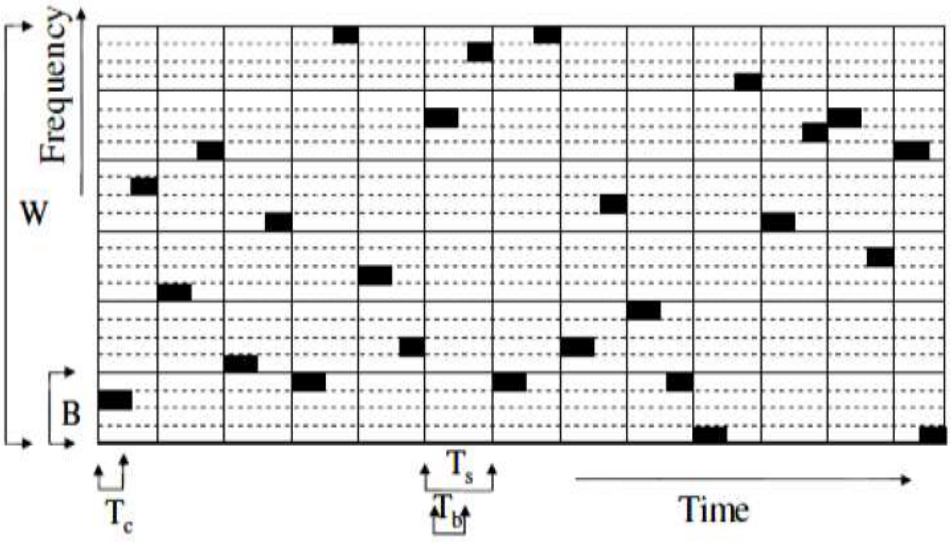

Fig 7.3: fast FHSS

7.3 Advantages of frequency hopping spread spectrum:

- **Processing gain:** in frequency hop system provides a large value processing gain which allows to process the signal with low signal to noise ratio at the receiver end.
- **Jamming resistance:** since a frequency hop signal generally has a lot of frequency slots, so the narrowband signal affects the signal only for a time period when signal hops to a carrier frequency jammed by the jammer.
- **Multiple access capability:** it can be used for multiple path environments as it can provide multiple accesses. Time division, frequency division and code division all can employ FHSS.
- **Short synchronization time:** FHSS system needs very short time for carrier synchronization which facilitates fast hopping making difficult to interfere or jam the signal
- **Multipath rejection:** for high hopping rate the receiver is tuned to another carrier frequency before the interference by a narrowband signal.

7.4 Spreading, modulation, dispreading & demodulation

Spreading code modulation: FHSS the frequency of carrier is hopped in a random manner known only to transmitter and receiver side. The number of frequency choices and the rate of hopping from frequency to frequency in any frequency hopper is governed by the requirements placed on it for a particular use. [9]

Process 2 – The message is modulated with a suitable carrier, but then we are transmitting the signal, with carrier frequency is being hopped in a specified manner.

Process -3: demodulation

After transmitting over the channel the modulated signal is demodulated using FSK demodulation using the same carrier and then de-spreaded and decoded by the receiver. [10].

It is the repeated switching of frequency which minimizes the unauthorized interception and jamming.

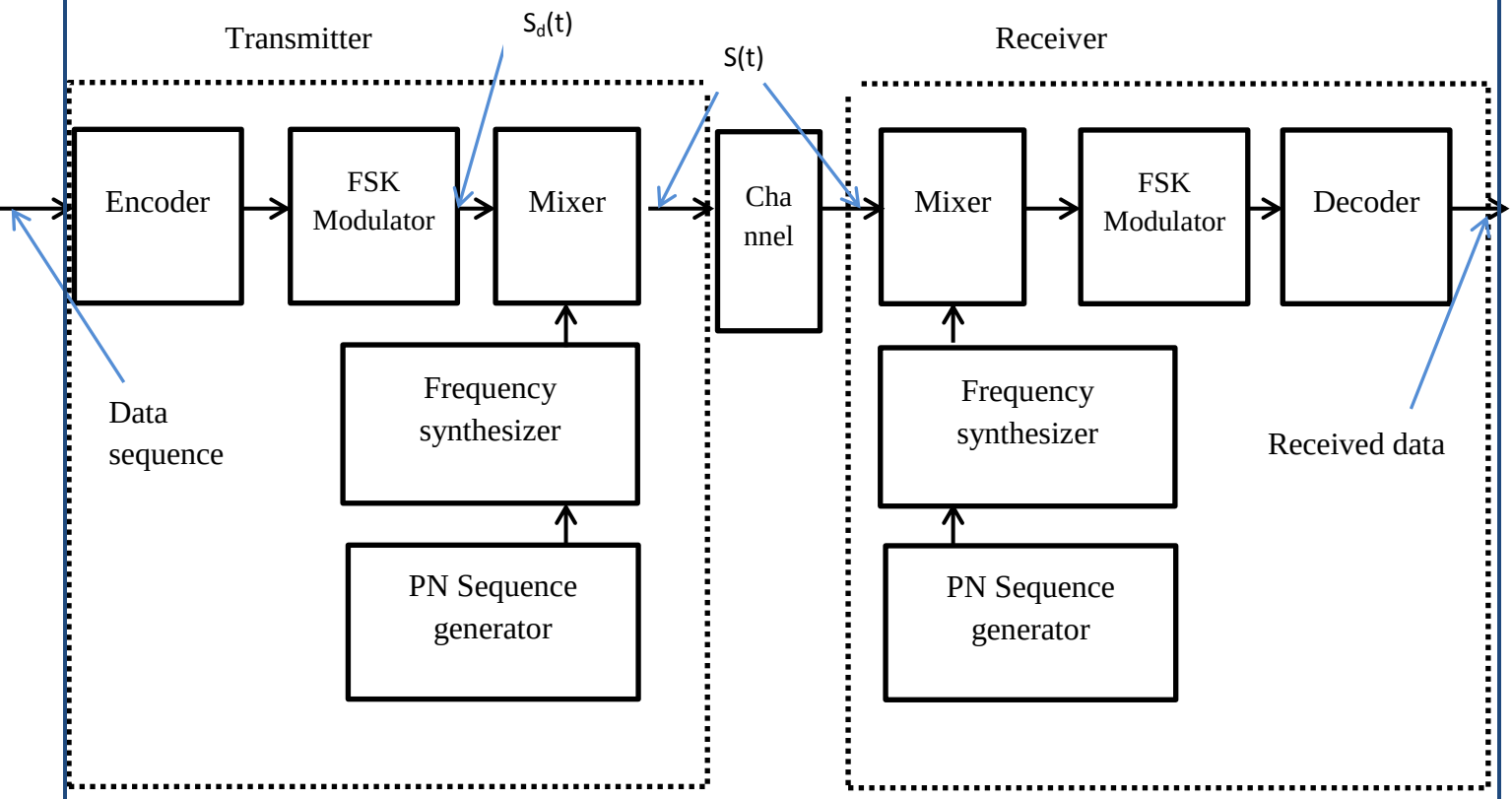

Fig 7.4: block diagram of FHSS

7.5 Difference between DSSS and FHSS

DSSS	FHSS
In DSSS system an interfering signal can overload the system and bring the entire system down.	This is more vulnerable to narrowband interference and noise than the DSSS system.
In order to implement a DSSS system linear modulation and class A or class AB amplification and i.e. radio power frequency amplification. And needs a nominal bandwidth 22Mhz bandwidth.[11]	This method is cheaper and easy to implement as it can use non-linear class C amplification and needs a nominal frequency of 1MHz.[11]
It is more useful in outdoor systems and non- cluttered environment.	This performs better in indoor systems and severe multipath environment. This is especially useful for portable devices.

CHAPTER 8

SIMULATION AND RESULTS:

8.1 DSSS Method

8.1.1 Signal without Noise

Enter the input Bits: [0 1 0 1 1 0 1 0 1 0]

Enter the length of each bit to be long 100

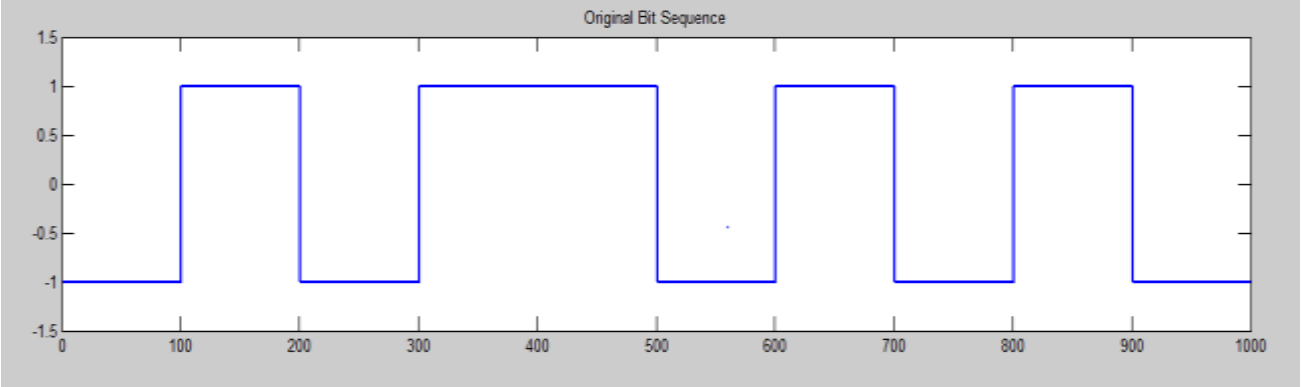

Fig 8.1.a

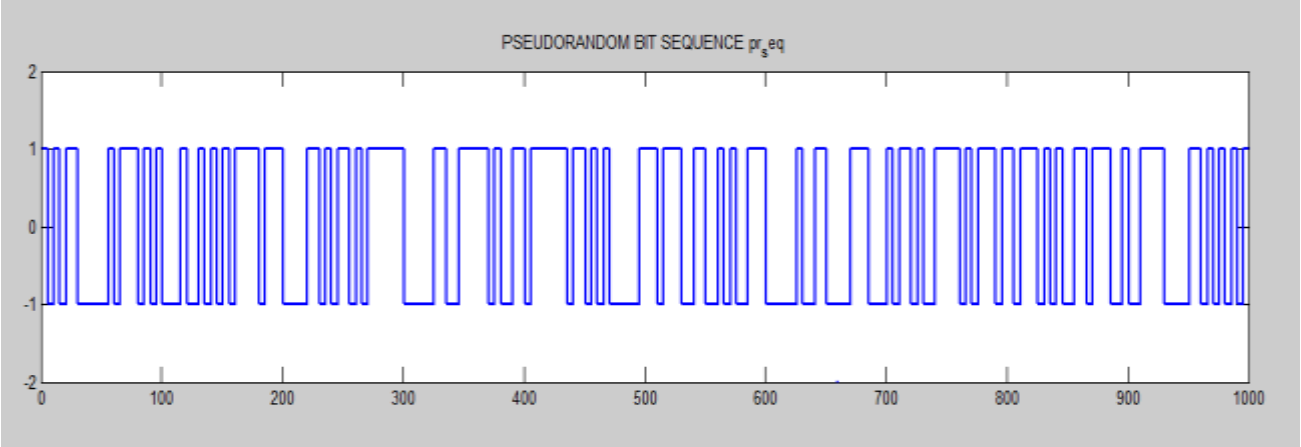

Fig 8.1.b

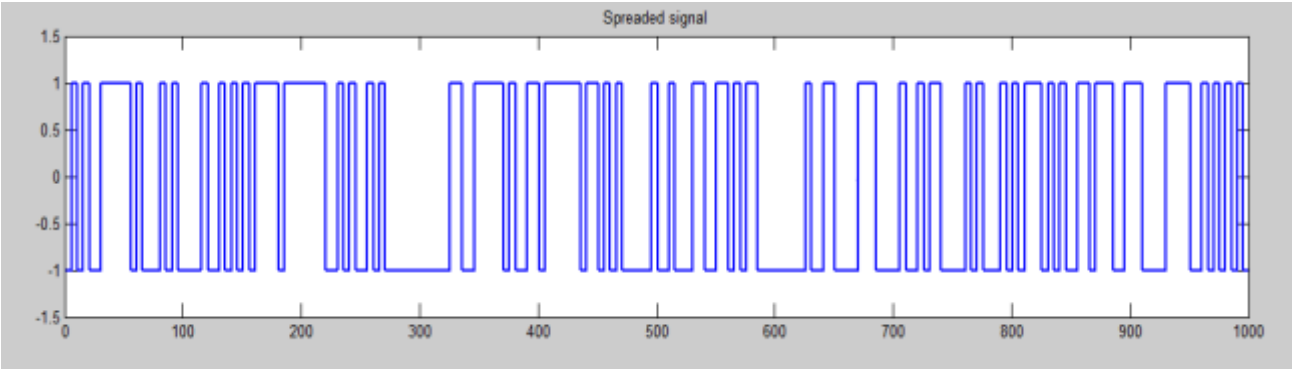

Fig 8.1.c

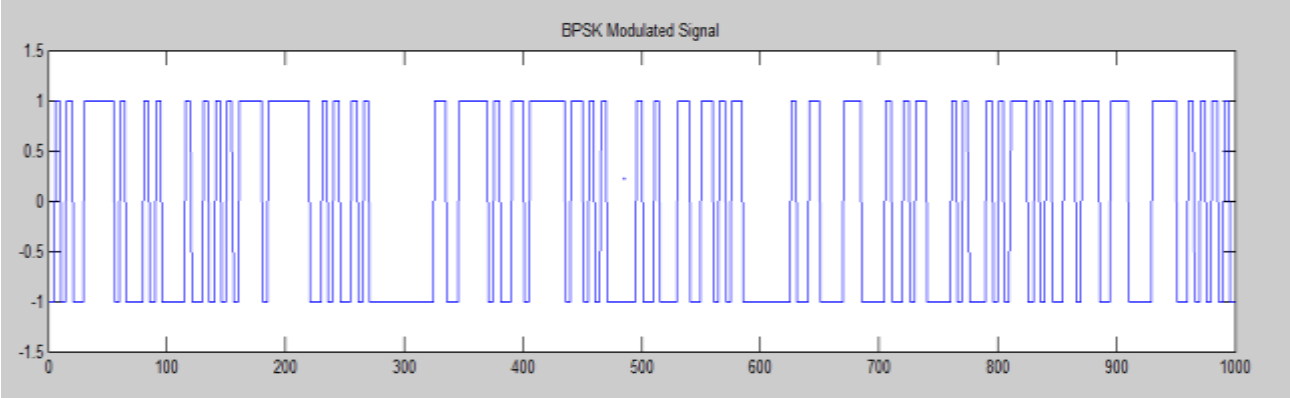

Fig 8.1.d

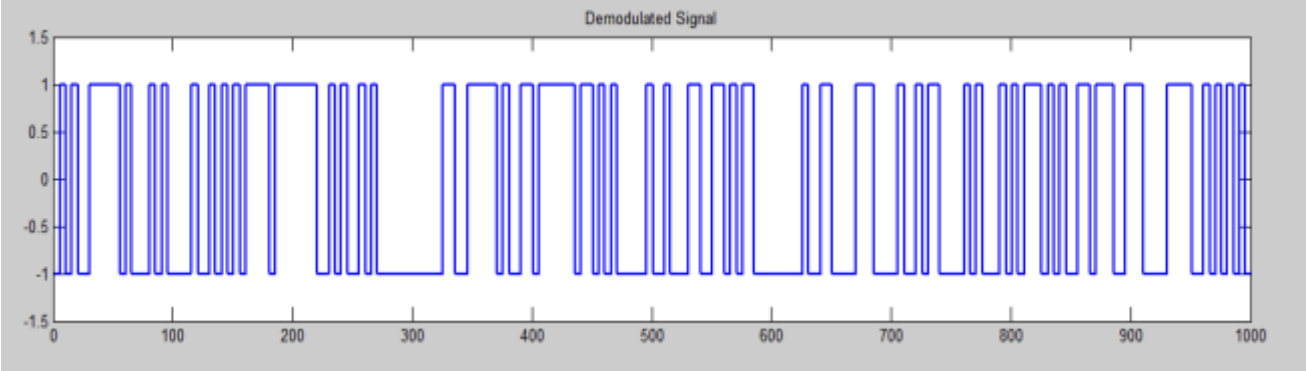

Fig 8.1.e

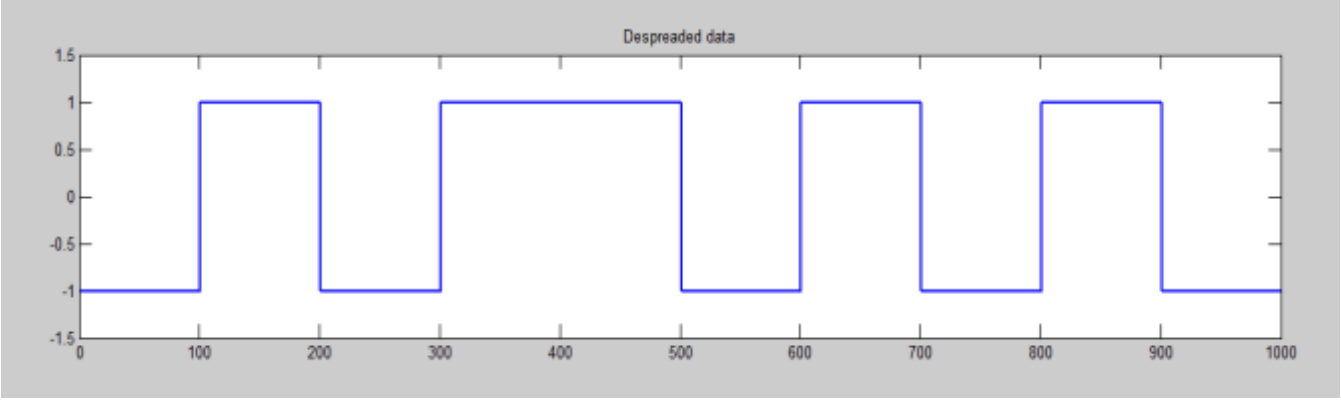

Fig 8.1.f

Fig 8.1: DSSS

8.2 Signal with noise

Enter the input Bits: [0 1 0 1 1 0 1 0 1 0]

Enter the length of each bit to be long 100

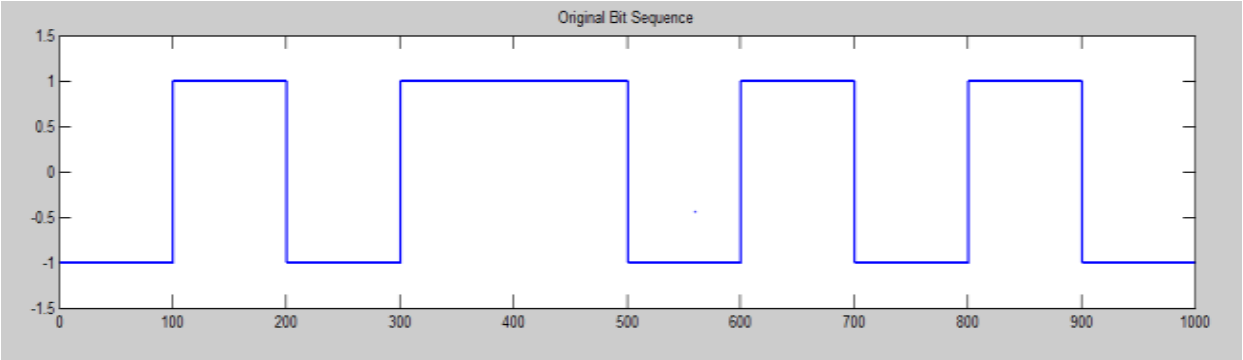

Fig 8.2.a

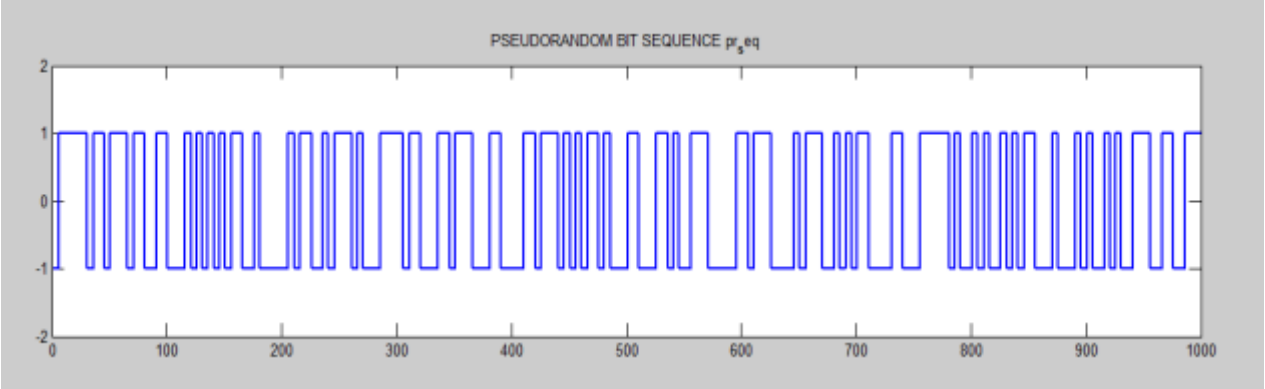

Fig 8.2.b

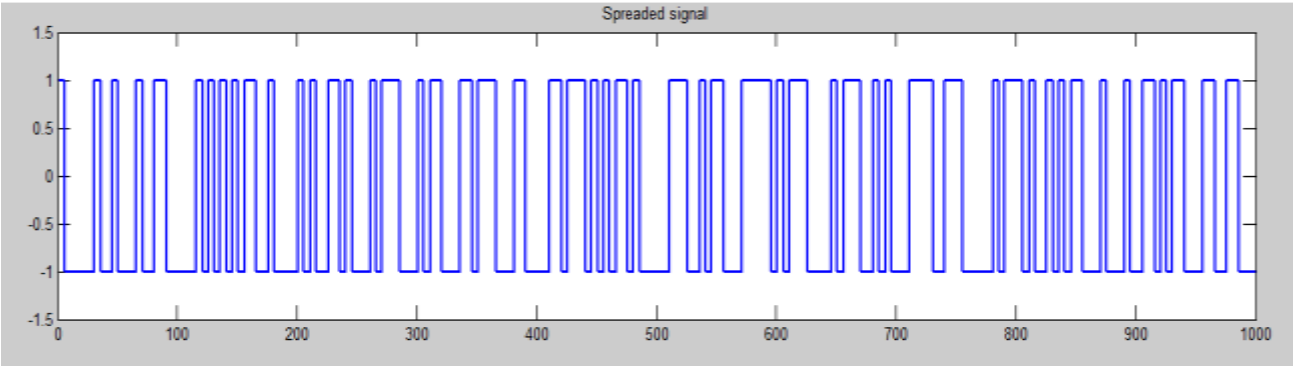

Fig 8.2.c

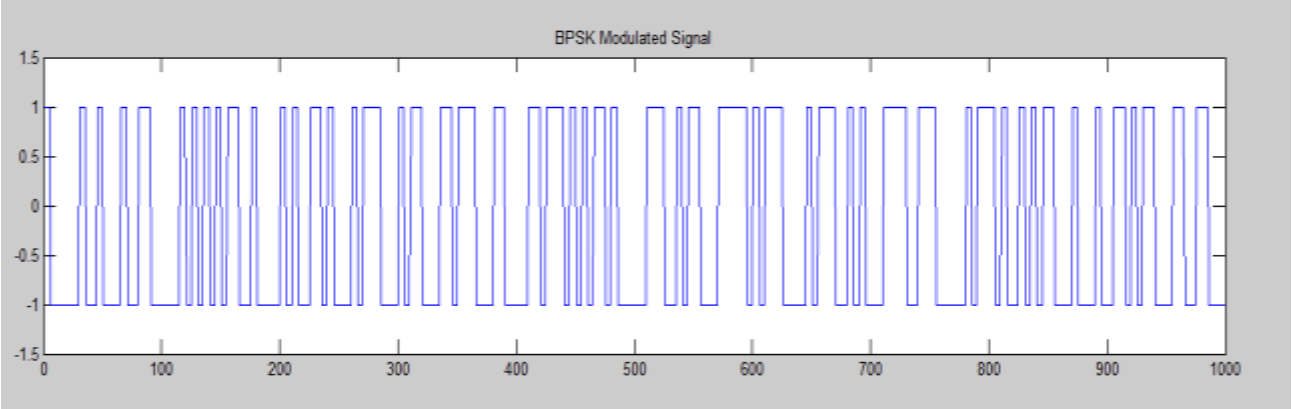

Fig 8.2.d

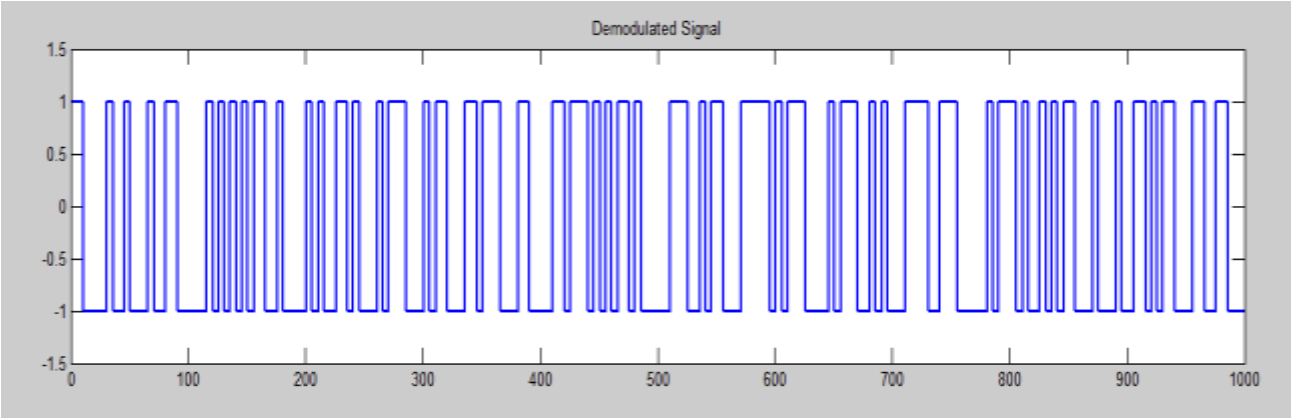

Fig 8.2.e

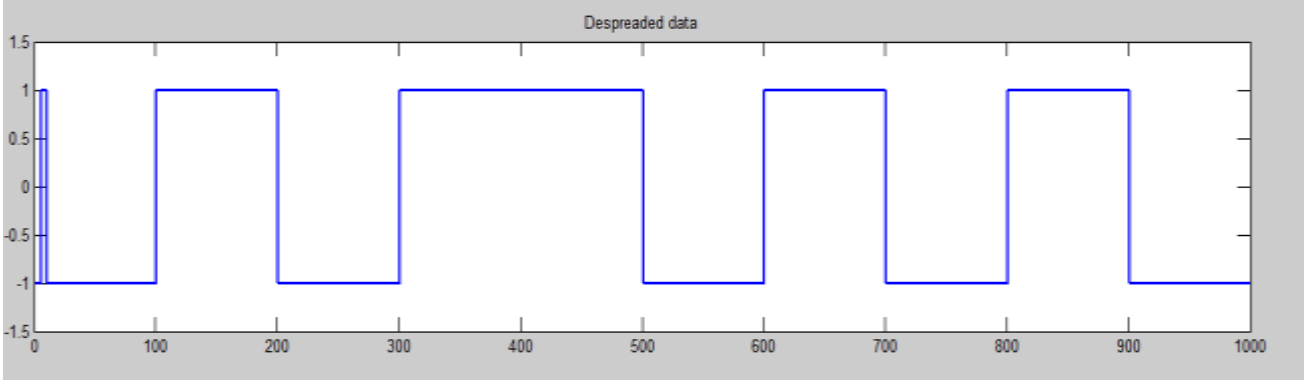

Fig 8.2.f

Fig 8.2: DSSS for signals with noise

8.3 Simulation output of FHSS

Transmitter side

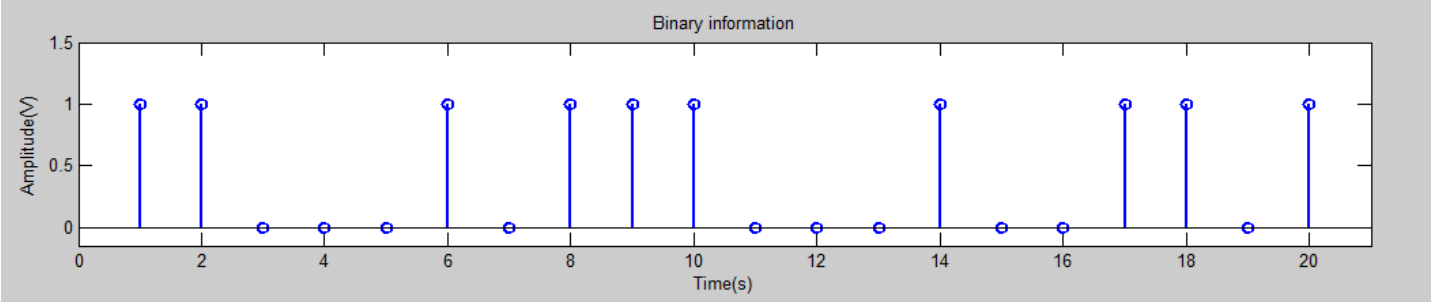

Fig 8.3.a

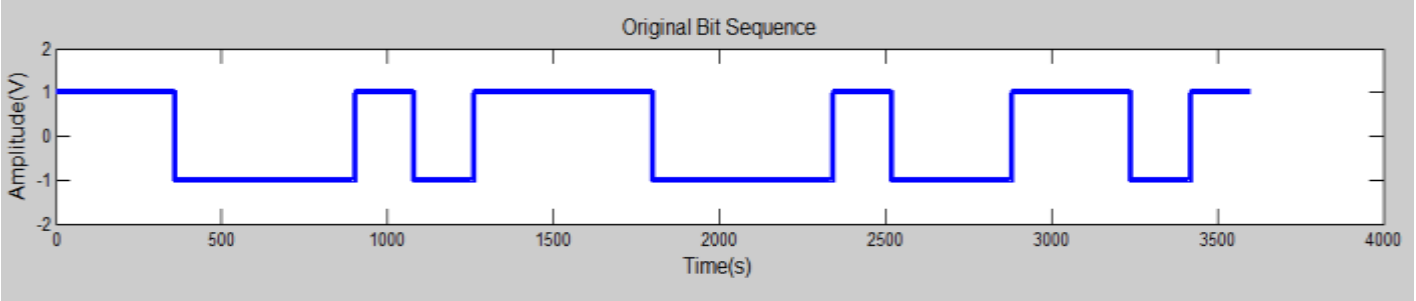

Fig 8.3.b

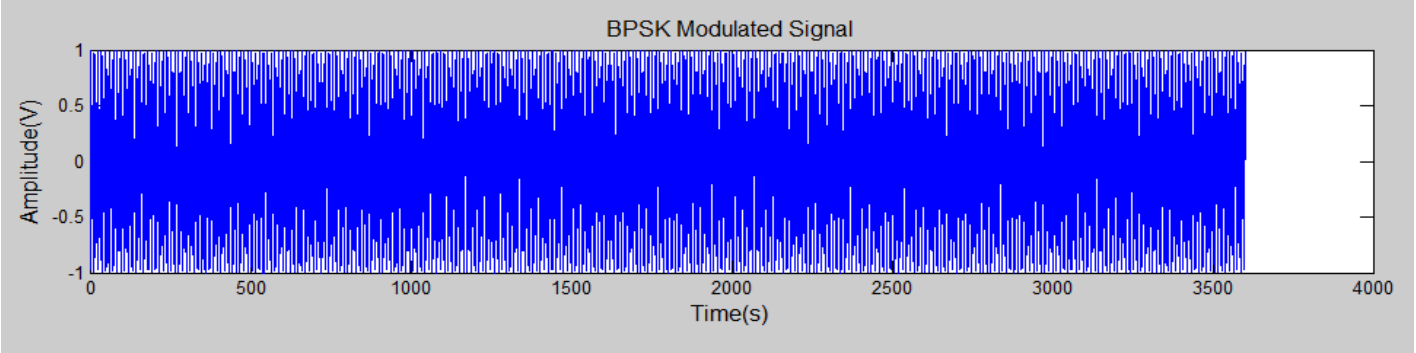

Fig 8.3.c

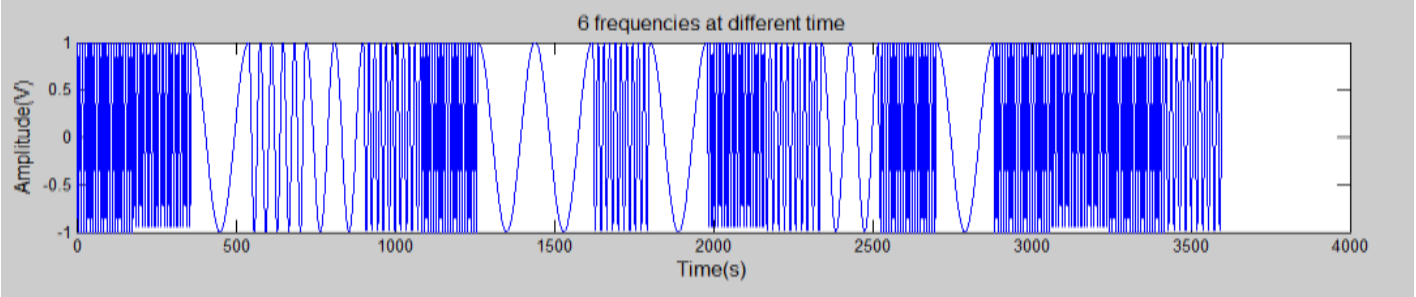

Fig 8.3.d

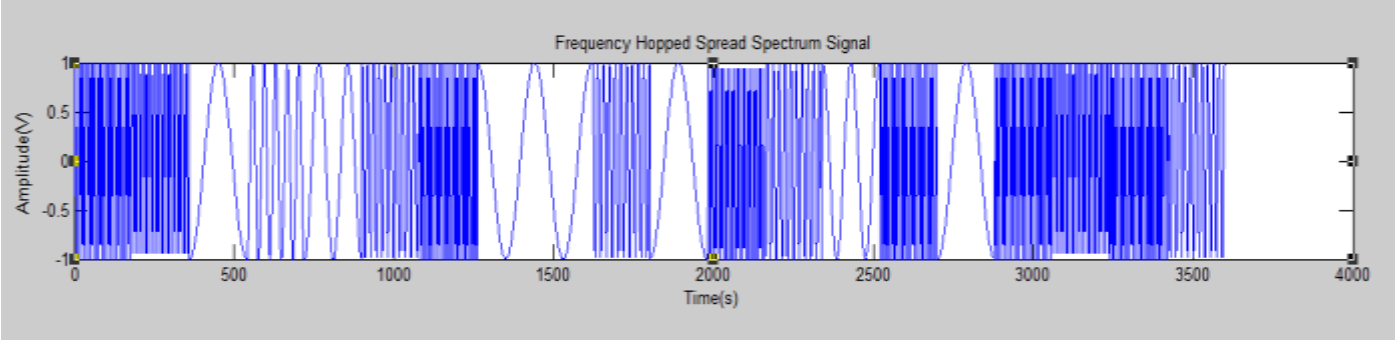

Fig 8.3.e

Receiver side

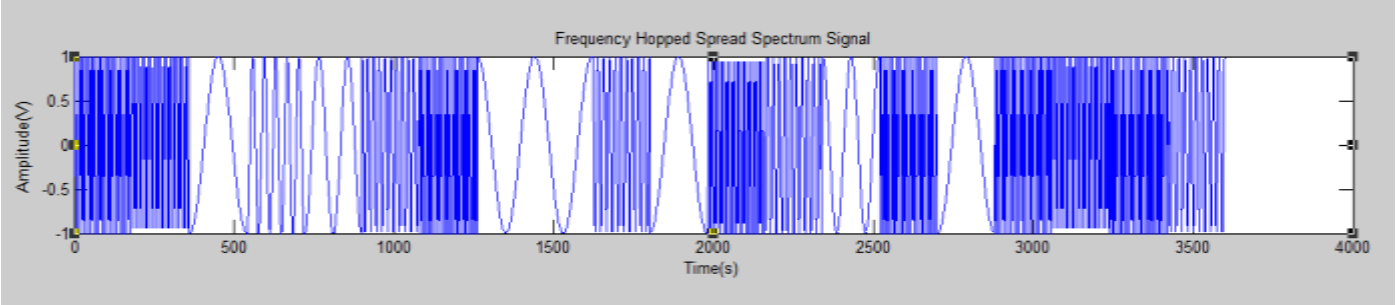

Fig 8.3.f

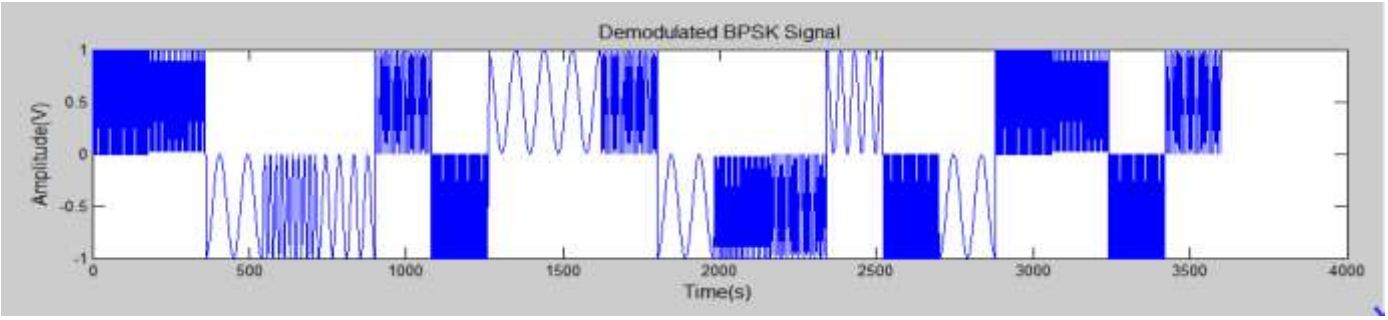

Fig 8.3.g

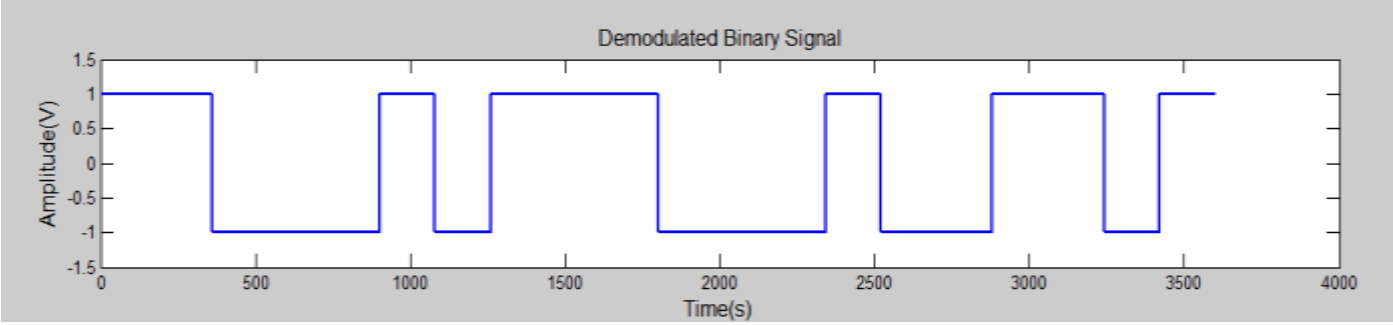

Fig 8.3.h

Fig 8.3: FHSS technique

CHAPTER 9

CONCLUSION

Smart Grid and Micro-grid are most advanced system in electrical power network. Smart-grid metering and control systems provide opportunity and technology for improving efficiency of the power system, convenience of distribution of electrical energy. In this paper we have introduced the spread spectrum technique for communication of the smart-grid so that the information can be transmitted securely and also shown test results for different methods available which allows us to conclude that both DSSS and FHSS methods can be employed for secured communication at the cost of some more infrastructure and technology and makes the overall cost a bit higher and highlighted several areas and directions for further research work. In India to implement Smart cities and Smart Grid proper use of security layer is also highly concern. We have mention some of security ideas in our project that will be helpful in deploying smart grid in near future.

10 REFERENCE

[1] Why smart grids? Abb.html www.newabb. Com

[2] www.globalsmartgridfederation.org/smartgrid/advantages

[3] Department of energy - USA U.S.Department of Energy by Litos Strategic Communication

[4] Spread Spectrum System with commercial application by Robert C. Dixon, 3rd Edition, A Wiley-Interscience Publication.

[5] Palak P.Parikh, Mitalkumar G kanbar and S.sindhu,"Opportunities and challenges of wireless communication Technologies for Smart Grid Applications", IEEE Power and Energy Society General Meeting. 2010.

[6] A.R Metke and R.L.Ekl."Security technology for Smart Grid Network",IEEE Trans. Smart Grid , vol 1 , no.1 ,june 2010,PP.99-107.

[7] Principles of Communication Systems by Herbert Taub and Donald L. Schilling, 2nd Edition, Tata McGraw- Hill Publication.

[8] Mike Mekkam, Reino Virrankoski,Mohammed Elmusrati Antila,"Communication System in Smart Grid Using Spectrum Sensing ",2013 IEEE 7th International Power Engineering and Optimisation Conference, 2013.

[9] Design and Simulation of Frequency Hopping Technique in Matlab

P. Olšovský, p. Podhoranský institute of electronics and photonics, faculty of electrical engineering and information technology, slovak university of technology

[10] V.C Gungor, B.Lu, and G.P Hancke,"Opportunities and challenges of Wireless Sensor networks in Smart grid", IEEE trans.Ind Electron vol.57, no.10, pp.3557-3564, oct 2010.

[11] FHSS Frequency Hopping Spread Spectrum, Farheen Bibi on April, 6th 2013 in Computing

[12] P.Palensky and D.Dietrich,"Demand Side Management: demand response, intelligent energy systems and smart load",IEEE trans.Ind Inform ,vol.7, no.3, pp.381-388,aug 2011.

[13] www.wikepedia.com/SmartGrid .